IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant(s): | W. Dale Hopkins, Steven W. Wierenga, Ching-Hsuan Chen, and Jack Schifando | | |
| Assignee: | Hewlett-Packard Development Company, L.P. | | |
| Title: | PIN VERIFICATION USING CIPHER BLOCK CHAINING | | |
| Serial No.: | 10/749,200 | Filing Date: | December 31, 2003 |
| Examiner: | Wang, Harris C | Group Art Unit: | 2139 |
| Docket No.: | 200309348-1 | Confirmation No.: | 9964 |

Irvine, California
March 18, 2008

**MAIL STOP AMENDMENT**
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

## REMARKS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

Dear Sir:

This paper is being filed with the Pre-Appeal Brief Request for Review responsive to the Final Office Action dated October 18, 2007, having a shortened statutory period expiring January 18, 2008. A 2-month petition for extension of time to respond is filed herewith setting a new period for response that expires March 18, 2008. Further examination and reconsideration are respectfully requested in view of the amendments and remarks set forth below.

## *OMISSION OF ESSENTIAL ELEMENTS REQUIRED TO ESTABLISH A PRIMA FACIE REJECTION*

### *Claim Rejections under 35 U.S.C. §112*

Claims 8, 16 and 24 rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicants believe "scanning" is an appropriate description of the sequential receipt of data, as described, but have amended the claims to replace "scanning" with "receiving in sequence" to possibly more correctly describe the operation. Applicants believe the amendment to be more descriptive of "scanning" than either "inputting" or "converting into digital data" as proposed by the Examiner and made the amendment to assist examination. Applicants believe the amendment is supported, for example in paragraphs [0008], [0009], and elsewhere. .

### *Rejection of Claims under 35 U.S.C. §103*

Claims 1-3, 7 and 9 are rejected under 35 U.S.C. §103(a) as being unpatentable over Coppersmith. Applicants' amended claims clarify that input text blocks are received by claimed structures rather than a capability of such receipt, thereby further distinguishing over Coppersmith. The Examiner admits that Coppersmith does not teach that the first input block is a text block contains a secret PIN, does not teach that the second input block is derived from a non-secret entity-identifier, and does not teach that the key is a Pin Verification Key. The Coppersmith disclosure neither describes nor even hints of receipt of the secret PIN and non-secret identity identifier, as claimed, to improve PIN verification.

*KSR International Co. v. Teleflex, Inc., et al., 550 U.S. ____, 127 S.Ct. 1727 (2007)* requires that an Examiner must provide "some articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness" (KSR opinion, page 14), and must "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed invention does" (KSR opinion, page 15).

The Examiner responds that impermissible hindsight was used since "the apparatus taught by Coppersmith was fully capable of receiving a PIN and a non-secret identity identifier." Such capability is irrelevant, since what is claimed is the particular handling of the PIN and the non-secret identifier, which is neither described nor hinted at by Coppersmith.

Applicants' amended Claim 3 clarifies that the apparatus operates in a reversible mode that actively recovers the secret PIN from the second ciphertext block. Claim 3 further distinguishes over Coppersmith which neither describes nor hints of recovery of the secret PIN as claimed or operation in the reversible mode.

Claims 4-5 are rejected under 35 U.S.C. §103(a) as being unpatentable over Coppersmith in view of Vernam (1310719). Applicants traverse the rejections. The Examiner admits that Coppersmith does not teach a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block, but states that Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext. Vernam does not teach first and second ciphertexts that are formed as specified in Claim 2 and combined to produce a ciphertext as in Claim 4, but rather merely discloses combination of a plaintext block with a ciphertext block. Accordingly, the combination of Coppersmith and Vernam does not combine signals and thus does not operate as claimed by the applicants. Regarding Claim 5, the combination of Coppersmith and Vernam neither describes nor hints of recovery of the secret PIN from the second ciphertext block as claimed or operation in the irreversible mode as claimed.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Vernam as applied to claim 5 above, and further in view of Briachtl. Claim 6 is patentable at least on the basis of depending from an allowable base claim.

Claims 8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Matyas. Applicants have amended Claim 8 to clarify that the format converter converts hexadecimal ciphertext to decimal. Claim 8 is patentable at least on the basis of depending from an allowable base claim but is further patentable because Coppersmith in view of Matyas do not disclose the format converter coupled to a cipher block in the CBC chain or generation of output digits as a PIN verification value, as claimed. The Examiner cites the lapse of time since discovery of pin verification (the late 1970's for IBM 3624) as motivation for making the combination. Applicants view such a lapse of time as irrelevant to motivation, but rather is an inference against obviousness since no such combination has been made since that time.

Regarding Claim 10, the Examiner admits that Coppersmith does not teach the first and second plaintext blocks as claimed but uses Matyas to justify such a format. The applicants traverse the rejection on the basis that Matyas does not disclose the plaintext block formats as claimed but merely gives definitions of the entities claimed by the applicants. Such definitions are not disputed to be known. What is novel and nonobvious is the connection of the plaintext blocks, as claimed, to improve PIN verification with the input application, as claimed, of the secret PIN and non-secret entity-identifier.

Claims 11-13, 16-21 and 24-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith. Applicants traverse the rejections. The Examiner admits Matyas does not teach a method of linking a plurality of cipher blocks, applying incoming plaintext blocks to cipher blocks, keying the cipher blocks with a key, XORing the plaintext block with an initialization vector, encrypting the initialized block using tripled DES encryption, XORing the plaintext block with the first ciphertext block, encrypting the chained block using triple DES encryption, and outputting the second cipher block. The Examiner uses Coppersmith to support elements that are missing from Matyas, however even combining Coppersmith with Matyas fails to disclose applying an incoming plaintext block derived fro a secret PIN to a cipher block, applying an incoming plaintext block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain, and keying the cipher blocks with a secret PVK.

The Examiner further admits that Coppersmith does not teach that the first input block that is a text block contains a secret PIN, does not teach that the second input block is derived from a non-secret entity-identifier, does not teach that the key is a Pin Verification Key, and does not teach that the output of the second ciphertext block is to be used for the purpose of PIN verification. Matyas similarly does not disclose application of a secret PIN and a non-secret identifier to a PIN verification system. The Examiner gives motivation for the combination that "Coppersmith without any modification can take the inputs of a secret PIN and the non-secret identifier and using a key output a Pin Verification Value." However, neither Matyas nor Coppersmith discloses application of the secret PIN and non-secret identifier to a PIN verification apparatus.

Regarding Claims 16 and 24, the claims are patentable at least on the basis of depending from an allowable base claim and are further patentable because Matyas in view of Coppersmith do not disclose the format converter coupled to a cipher block in the CBC chain or generation of output digits as a PIN verification value, as claimed. The Examiner cites the lapse of time since discovery of pin verification (the late 1970's for IBM 3624) as motivation for making the combination. Applicants view such a lapse of time as irrelevant to motivation or actually evidence against motivation since no such combination has been made since that time.

Regarding Claims 17 and 25, the claims are patentable at least on the basis of depending from an allowable base claim.

Regarding Claims 19 and 27, the claims are patentable at least on the basis of depending from an allowable base claim and are further patentable because Matyas in view of Coppersmith do not disclose first and second plaintext blocks in the format as claimed.

The applicants traverse the rejection on the basis that Matyas does not disclose the plaintext block formats as claimed but merely gives definitions of the entities claimed by the applicants. Such definitions are not disputed to be known. What is novel and nonobvious is the connection of the plaintext blocks, as claimed, to improve PIN verification.

Claims 14 and 22 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas in view of Coppersmith as applied to claims 11 and 20 above, and further in view of Vernam. Applicants traverse the rejections. Claims 14 and 22 are patentable at least on the basis of depending from an allowable base claim and are further patentable because Vernam does not teach first and second ciphertexts that are combined to produce a ciphertext, but rather discloses combination of a plaintext block with a ciphertext block. Accordingly, the combination of Matyas, Coppersmith, and Vernam does not operate as claimed by the applicants.

Claims 15 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith further in view of Vernam as applied to claims 14 and 22 above, and further in view of Brachtl. Claims 15 and 23 are allowable at least on the basis of depending from allowable base claims.

## CONCLUSION

The application, including all remaining Claims 1-31, is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at (949) 251-0250.

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, Central Number at (571) 273-8300 on the date shown below:

(Signature)

Joy C. Ngo
(Printed Name of Person Signing Certificate)

March 18 2008
(Date)

Respectfully submitted,

Ken J. Koestner
Attorney for Applicant(s)
Reg. No. 33,004

KOESTNER BERTANI LLP

2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x OMB 0651-00xx
U S Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

| | | |
|---|---|---|
| **PRE-APPEAL BRIEF REQUEST FOR REVIEW** | Docket Number (Optional)<br>200309348-1 | |
| I hereby certify that this correspondence is being facsimile transmitted to the USPTO, Central Number at (571) 273-8300 on the date shown below:<br>on March 18, 2008<br>Signature<br>Typed or printed name Joy C. Ngo | Application Number<br>10/749,200 | Filed<br>December 31, 2003 |
| | First Named Inventor<br>W. Dale Hopkins | |
| | Art Unit<br>2139 | Examiner<br>Wang, Harris C |

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 33,004

□ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1 34 ________

Signature

Ken J. Koestner
Typed or printed name

(949) 251-0250
Telephone number

March 18, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*

□ *Total of ________ forms are submitted.

This collection of information is required by 35 U.S.C 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application Confidentiality is governed by 35 U S C. 122 and 37 CFR 1 11, 1 14 and 41 6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U S. Department of Commerce, P O Box 1450, Alexandria, VA 22313-1450 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*